Deloitte.

TECHNICAL RESPONSE PACKET
710-24-0002
(REDACTED COPY)

RESPONSE SIGNATURE PAGE

Type or Print the following information.

[redacted]

SECTIONS 1 – 4: VENDOR AGREEMENT AND COMPLIANCE

- *Any requested exceptions to items in this section which are NON-mandatory **must** be declared below or as an attachment to this page. Vendor **must** clearly explain the requested exception, and should label the request to reference the specific solicitation item number to which the exception applies.*
- *Exceptions to Requirements **shall** cause the vendor's proposal to be disqualified.*

[redacted]

By signature below, vendor agrees to and **shall** fully comply with all Requirements as shown in this section of the bid solicitation.

Authorized Signature: [redacted]

Printed/Typed Name: [redacted]

State of Arkansas
DEPARTMENT OF HUMAN SERVICES
700 South Main Street
P.O. Box 1437 / Slot W345
Little Rock, AR 72203

ADDENDUM 1

TO: All Addressed Vendors
FROM: Office of Procurement
DATE: January 17, 2024
SUBJECT: 710-24-0002 Arkansas Health Insurance Premium Payment (ARHIPP)

The following change(s) to the above referenced RFP have been made as designated below:

_____Change of specification(s)
_____ Additional specification(s)
_____ Change of bid opening date and time
_____ Cancellation of bid
__X____ Other

OTHER

- Attachment I - Remove and replace with Attachment I Revised Client History Form.
- Cost Proposal Template – remove and replace with Attachment K Revised Cost Proposal Template
- Section 1.32 of the solicitation Schedule of Events – remove and replace the Go Live Date, with the following: On or About September 1, 2024
- Section 2.2.D – remove and replace with the following:

  The Contractor shall have at least five (5) years cumulative experience working on similar insurance contracts for at least three (3) other state Medicaid programs. If the Prospective Contractor proposes to use subcontractors, the Prospective Contractor's proposed subcontractors shall have the experience working on similar projects with other State Medicaid programs. For verification purposes, the Prospective Contractor must accurately complete and sign Attachment I – Revised Client History Form.

The specifications by virtue of this addendum become a permanent addition to the above referenced RFP. Failure to return this signed addendum may result in rejection of your proposal.

If you have any questions, please contact: Karrie Goodnight, DHS.OP.Solicitations@dhs.arkansas.gov, 501-320-3906.

[redacted] [redacted]

Vendor Signature Date

Deloitte Consulting LLP

Company

CONTRACT AND GRANT DISCLOSURE AND CERTIFICATION FORM

Failure to complete all of the following information may result in a delay in obtaining a contract, lease, purchase agreement, or grant award with any Arkansas State Agency.

SUBCONTRACTOR: ☐ Yes ☒ No SUBCONTRACTOR NAME:

TAXPAYER ID NAME: Deloitte Consulting LLP IS THIS FOR: ☐ Goods? ☒ Services? ☐ Both?

YOUR LAST NAME: [redacted] M.I.:

ADDRESS: 400 W Capitol Avenue, Suite 900

CITY: Little Rock STATE: AR ZIP CODE: 72201 COUNTRY: USA

AS A CONDITION OF OBTAINING, EXTENDING, AMENDING, OR RENEWING A CONTRACT, LEASE, PURCHASE AGREEMENT, OR GRANT AWARD WITH ANY ARKANSAS STATE AGENCY, THE FOLLOWING INFORMATION MUST BE DISCLOSED:

FOR INDIVIDUALS*

Indicate below if: you, your spouse or the brother, sister, parent, or child of you or your spouse *is* a current or former: member of the General Assembly, Constitutional Officer, State Board or Commission Member, or State Employee:

Position Held	Mark (√)		Name of Position of Job Held [senator, representative, name of board/ commission, data entry, etc.]	For How Long?		What is the person(s) name and how are they related to you? [i.e., Jane Q. Public, spouse, John Q. Public, Jr., child, etc.]	
	Current	Former		From MM/YY	To MM/YY	Person's Name(s)	Relation
General Assembly							
Constitutional Officer							
State Board or Commission Member							
State Employee							

☒ **None of the above applies**

FOR AN ENTITY (BUSINESS)*

Indicate below if any of the following persons, current or former, hold any position of control or hold any ownership interest of 10% or greater in the entity: member of the General Assembly, Constitutional Officer, State Board or Commission Member, State Employee, or the spouse, brother, sister, parent, or child of a member of the General Assembly, Constitutional Officer, State Board or Commission Member, or State Employee. Position of control means the power to direct the purchasing policies or influence the management of the entity.

Position Held	Mark (√)		Name of Position of Job Held [senator, representative, name of board/commission, data entry, etc.]	For How Long?		What is the person(s) name and what is his/her % of ownership interest and/or what is his/her position of control?		
	Current	Former		From MM/YY	To MM/YY	Person's Name(s)	Ownership Interest (%)	Position of Control
General Assembly								
Constitutional Officer								
State Board or Commission Member								
State Employee								

☒ **None of the above applies**

Contract and Grant Disclosure and Certification Form

Failure to make any disclosure required by Governor's Executive Order 98-04, or any violation of any rule, regulation, or policy adopted pursuant to that Order, shall be a material breach of the terms of this contract. Any contractor, whether an individual or entity, who fails to make the required disclosure or who violates any rule, regulation, or policy shall be subject to all legal remedies available to the agency.

As an additional condition of obtaining, extending, amending, or renewing a contract with a *state agency* I agree as follows:

1. Prior to entering into any agreement with any subcontractor, prior or subsequent to the contract date, I will require the subcontractor to complete a **CONTRACT AND GRANT DISCLOSURE AND CERTIFICATION FORM**. Subcontractor shall mean any person or entity with whom I enter an agreement whereby I assign or otherwise delegate to the person or entity, for consideration, all, or any part, of the performance required of me under the terms of my contract with the state agency.

2. I will include the following language as a part of any agreement with a subcontractor:

   Failure to make any disclosure required by Governor's Executive Order 98-04, or any violation of any rule, regulation, or policy adopted pursuant to that Order, shall be a material breach of the terms of this subcontract. The party who fails to make the required disclosure or who violates any rule, regulation, or policy shall be subject to all legal remedies available to the contractor.

3. No later than ten (10) days after entering into any agreement with a subcontractor, whether prior or subsequent to the contract date, I will mail a copy of the **CONTRACT AND GRANT DISCLOSURE AND CERTIFICATION FORM** completed by the subcontractor and a statement containing the dollar amount of the subcontract to the state agency.

I certify under penalty of perjury, to the best of my knowledge and belief, all of the above information is true and correct and that I agree to the subcontractor disclosure conditions stated herein.

Signature [redacted] Title [redacted] Date 01/30/2024

Vendor Contact Person [redacted] Title [redacted] Phone No. [redacted]

Agency use only

Agency Number_____ Agency Name_____ Agency Contact Person_____ Contact Phone No._____ Contract or Grant No._____

Deloitte.

Deloitte
30 Rockefeller Plaza
New York
USA

Tel: 212-492-4000
Fax: 212-489-1687
www.deloitte.com

AFFIRMATIVE ACTION FOR EQUAL EMPLOYMENT OPPORTUNITY – A STATEMENT OF POLICY

[redacted]

Affirmative Action Plans

The Office of Federal Contract Compliance Programs (OFFCP) requires that Deloitte prepare affirmative action plans and update them annually. Deloitte's plans incorporate the policies referenced herein and also specify the actions to be taken if the policies are not adhered to. Employees may request access to these plans by contacting Talent ELE Compliance.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

PROPOSED SUBCONTRACTORS FORM

• ***Do not*** *include additional information relating to subcontractors on this form or as an attachment to this form.*

PROSPECTIVE CONTRACTOR PROPOSES TO USE THE FOLLOWING SUBCONTRACTOR(S) TO PROVIDE SERVICES.

Type or Print the following information

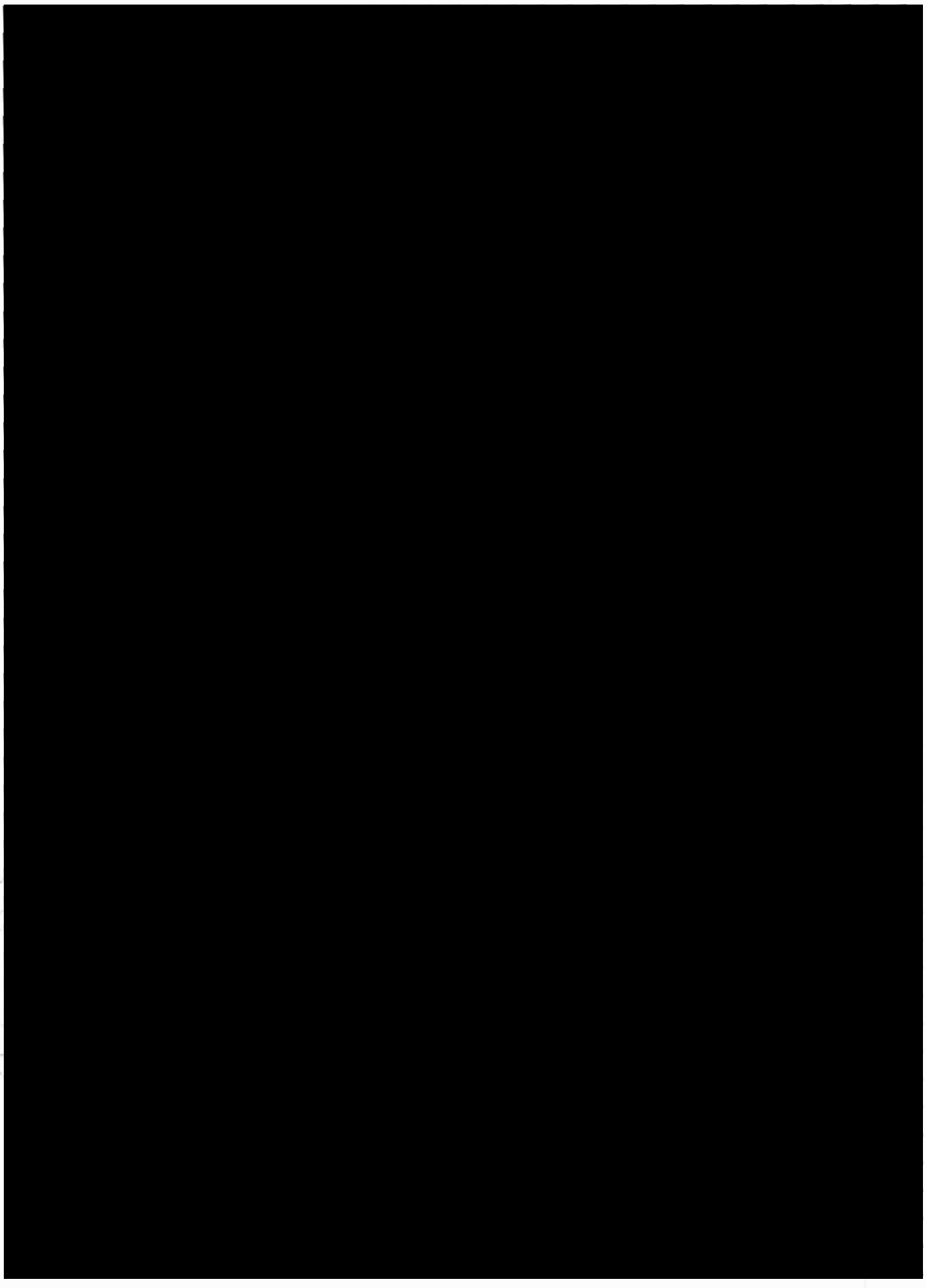
Subcontractor's Company Name	Street Address	City, State, ZIP

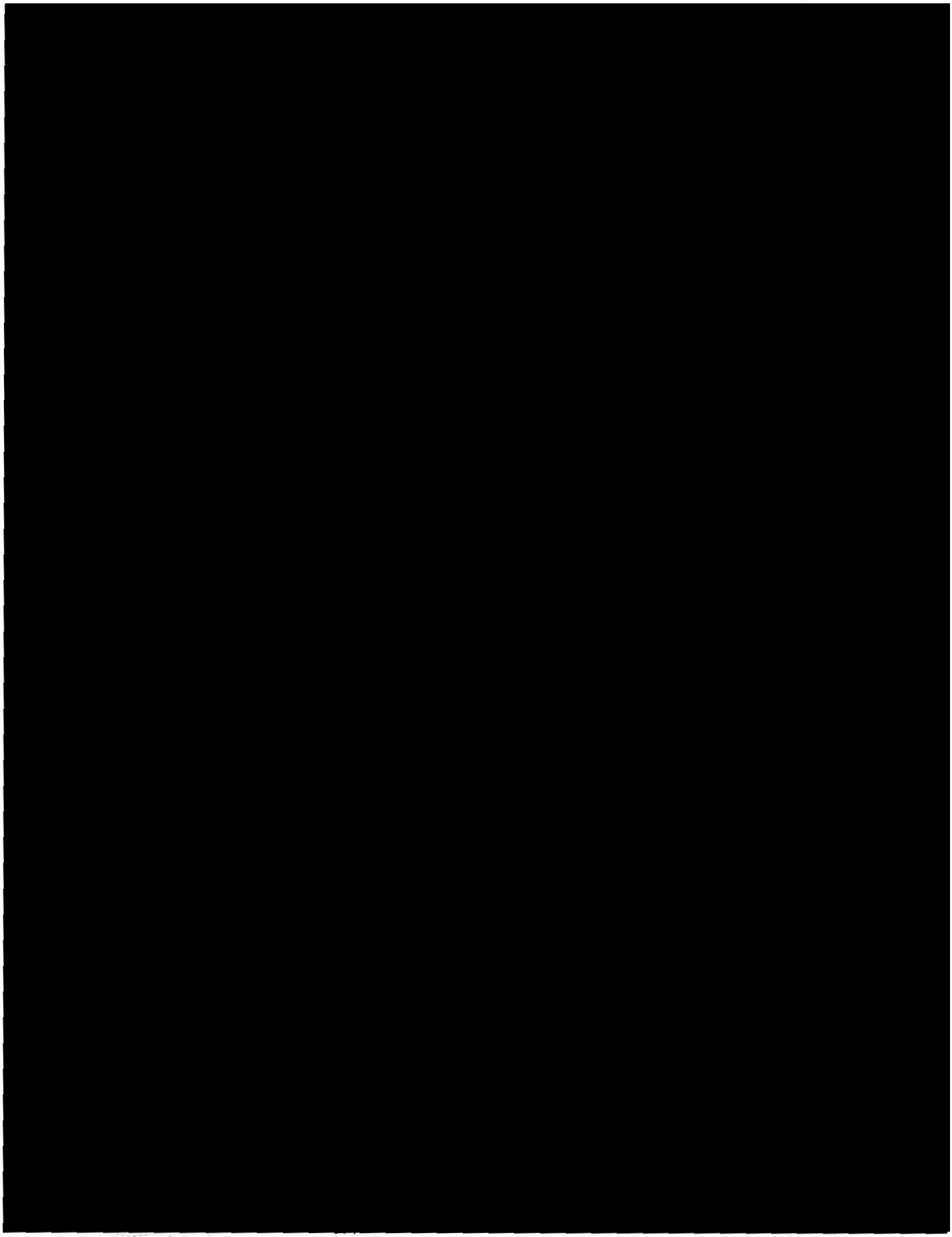
☒ PROSPECTIVE CONTRACTOR DOES NOT PROPOSE TO USE SUBCONTRACTORS TO PERFORM SERVICES.

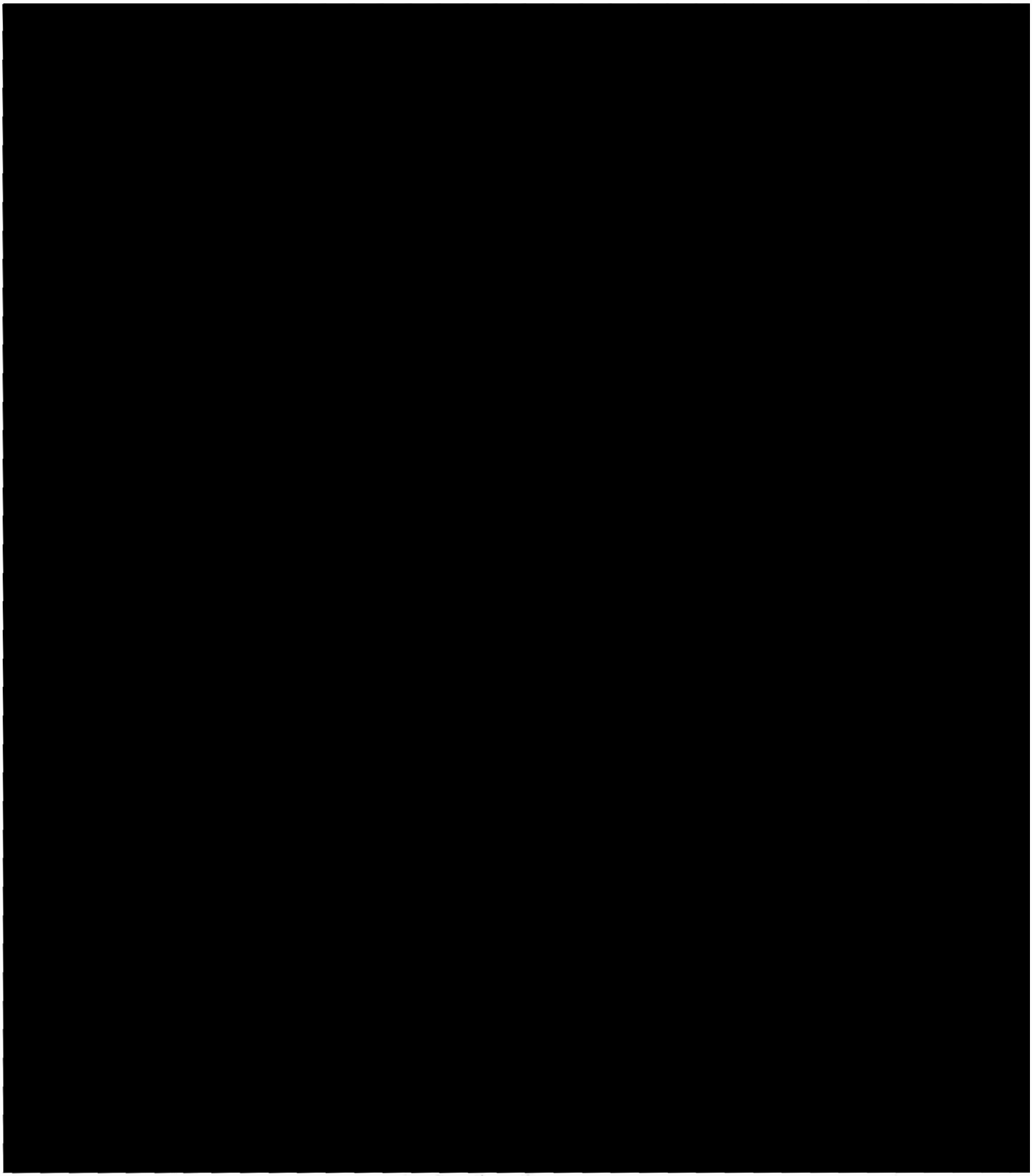
Deloitte.

Other Documents
710-24-0002

TRAVELERS







AR DHS-OIT- Standard IT Requirements Approved by Enterprise Architecture Board.

Document Version 1.3

Change History

Date	Version	Notes
8/1/2019		Initial draft
8/22/2019	1.0	First Version
9/26/2019		updated for ACS requirements
12/16/2019	1.2	Updated version (Minor changes)
1/31/2020	1.3	Updated in Jan 2020.Document updated to be used in 2020 after presenting to EAB.

Requirement Number	Requirement Group	Requirement Subgroup	Requirement	Comments	Meets Requirements	Describe How Requirements Met
1	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall develop, document and manage the processes and procedures for Interfaces and Batch Operations Architecture.	NA	Yes	[redacted]
2	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall define job scheduling requirements, application software interdependencies, and rerun requirements for all production jobs	NA	Yes	[redacted] landscapes, our commitment extends to continuous improvement by Regular Reviews, Feedback Mechanisms, Adaptability.
3	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall utilize and manage scheduling tools for automating job execution (e.g., job workflow processes interdependencies, rerun requirements, file exchange functions, and print management)	NA	Yes	[redacted]

4	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall maintain a master job schedule and execute all batch jobs for the DHS Enterprise Program (e.g. any jobs provided by any vendor working on/with the DHS Enterprise Platform)	NA	Yes	[redacted]
5	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall perform job monitoring and manage resolution of any failed jobs.	NA	Yes	[redacted]
6	Application Hosting	Change/Release Management	Any technology vendor, application or solution shall adhere to the Information Technology Infrastructure Library (ITIL) V3.0 Change and Release Management processes.	NA	Yes	[redacted]
7	Application Hosting	Change/Release Management	Any technology vendor, application or solution shall identify and submit any changes in compliance with the DHS Enterprise Program Change/Release Management process.	NA	Yes	[redacted]
8	Application Hosting	Disaster Recovery	Any technology vendor, application or solution shall maintain a detailed Disaster Recovery plan to meet Disaster Recovery requirements. Plan shall include plans for data, back-ups, storage management, and contingency operations that provides for recovering the DHS Enterprise Platform within established recovery requirement timeframes after a disaster that has affected the users of the DHS Enterprise Platform.	NA	Yes	[redacted]

9	Application Hosting	Disaster Recovery	Any technology vendor, application or solution shall provide support to the DHS support teams with implementing, configuring and testing disaster recovery.	NA	Yes	[redacted]
10	Application Hosting	Disaster Recovery	Any technology vendor, application or solution shall develop action plans to address any issues arising from Disaster Recovery testing.	NA	Yes	[redacted]
11	Application Hosting	Infrastructure Security	Any technology vendor, application or solution using cloud technology shall be located within the continental US. All servers and data will be located in US Soil.	NA	Yes	[redacted]
12	Application Hosting	Infrastructure Security	Any technology vendor, application or solution shall proactively monitor all infrastructure including but not limited to network, storage, virtual environments, servers, databases, firewalls, etc. following industry best practices.	NA	Yes	[redacted]
13	Application Hosting	Infrastructure Security	Any technology vendor, application or solution shall implement physical and logical security within new functionality defined in the security plan consistent with DHS' security policies and industry standards.	NA	Yes	[redacted]
14	Application Hosting	Infrastructure Security	Any technology vendor, application or solution shall review all available infrastructure security patches relevant to the environment and classify the need and speed in which the security patches should be installed as defined by DHS security policies.	NA	Yes	[redacted]

15	Application Hosting	Network, Hosting and Data Center Services	Any technology vendor, application or solution shall provision new environments and capacity as required to ensure performance requirements are met as volume increases and additional functionality is implemented.	NA	Yes	[redacted]
16	Application Hosting	Operating System, Application and Database Backup and Recovery	Any technology vendor, application or solution shall encrypt all data at rest including backups using DHS and regulatory bodies (CMS, FNS, etc.) standards regardless of storage media.	NA	Yes	[redacted]
17	Application Hosting	Storage Management Services	Any technology vendor, application or solution will provide data backup and restoration services in accordance with industry best practices.	NA	Yes	[redacted]
18	Application Hosting	Storage Management Services	Any technology vendor, application or solution will recommend techniques and procedures to ensure disk storage resources are utilized in an efficient and cost-effective manner.	NA	Yes	[redacted]
19	Application Hosting	Storage Management Services	Any technology vendor, application or solution shall regularly test recovery procedures and practices to demonstrate recoverability and verify that actual practices are in concert with procedures and report results, as well as meet business requirements	NA	Yes	[redacted]
20	Application Hosting	Storage Management Services	Any technology vendor, application or solution shall monitor and demonstrate compliance with Arkansas Records Retention Schedule.	NA	Yes	[redacted]

21	Application Hosting	System Monitoring	Any technology vendor, application or solution shall manage and maintain monitoring procedures and standards for system/solution/infrastructure including, but not limited to: a. Monitoring of buffers, database buffers, table space fragmentation, database space, for unusual growth and propose a solution in case of alert b. Monitoring of system logs, update error, database corruption, jobs execution failures etc. and propose solution in case of an alert c. Monitoring of alert notification interface (e.g.,	NA	Yes	[redacted]
22	Application Hosting	System Monitoring	Any technology vendor, application or solution shall monitor infrastructure for availability as well as transaction and response time performance.	NA	Yes	[redacted]
23	Application Hosting	System Monitoring	Any technology vendor, application or solution shall provide regular monitoring reports of infrastructure performance, utilization and efficiency (e.g., proactive system monitoring)	NA	Yes	[redacted]
24	Application M&O Services	Disaster Recovery	Any technology vendor, application or solution shall identify and make available appropriate resources to support DHS' disaster recovery planning, testing and execution.	NA	Yes	[redacted]
25	Application M&O Services	Security Administration	Any technology vendor, application or solution shall provide documented procedures for security monitoring and log management functions, and use write-once technology or other secure approaches for storing audit trails and security logs.	NA	Yes	[redacted]

26	Data Governance	Master Data Management	Any technology vendor, application or solution shall provide data dictionary, data models, data flow models, process models and other related planning and design documents to DHS.	NA	Yes	[redacted]
27	General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution shall maintain a record (e.g. audit trail) of all additions, changes and deletions made to data in the applicable system or solution. In addition, a log of query or view access to certain type of records and/or screens will be maintained for investigative purposes. This should be readily searchable by user ID or client ID. This must include, but is not limited to: a. The user ID of the person who made the change b. The date and time of the change c. The physical, software/hardware and	NA	Yes	[redacted]
28	General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution shall prevent modifications to the audit records.	NA	Yes	[redacted]
29	General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution must have the ability to capture electronic signatures on all documents, forms, letters, and correspondences.	NA	Yes	[redacted]

30	General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution shall be able to detect security-relevant events (as defined in NIST 800-53 moderate baseline, rev 4) that it mediates and generate audit records for them. At a minimum the events will include, but not be limited to: a. Start/stop b. User login/logout c. Session timeout d. Account lockout e. Client record created/viewed/updated/deleted f. Scheduling g. Query h. Order i. Node-authentication failure	NA	Yes	[redacted]
31	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution interfaces will secure and protect (encrypt) the data and the associated infrastructure from a confidentiality, integrity and availability perspective.	NA	Yes	[redacted]
32	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall develop/integrate services using standardized Web Services formats.	NA	Yes	[redacted]
33	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall provide the ability to publish services and related data to be used by different types and classes of service consumers.	NA	Yes	[redacted]

34	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall provide the capabilities for a Real-Time (or near real-time) Integrated Enterprise where common data elements about the customers served (e.g., clients) and services rendered are easily shared across organizational units with appropriate adherence to State and Federal security and privacy restrictions.	NA	Yes	[redacted]
35	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have the capability to implement synchronous and asynchronous program-to-program communication, moving messages between service oriented architecture (SOA) service consumer modules and service provider modules at runtime.	NA	Yes	[redacted]
36	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have message and data formats that will be based on logical representations of business objects rather than native application data structures.	NA	Yes	[redacted]
37	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall avoid point-to-point integrations. Application integration, both internal and external, will go through the DHS Enterprise Service Bus/Data Integration Hub.	NA	Yes	[redacted]
38	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution WSDLs developed for Arkansas will conform to the W3C standards for restful API development.	NA	Yes	[redacted]

39	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution design will allow for the solution to continue to operate despite failure or unavailability of one or more individual technology solution components.	NA	Yes	[redacted]
40	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have the ability to use standards-based communication protocols, such as TCP/IP, HTTP, HTTP/S and SMTP. Protocol bridging: The ability to convert between the protocol native to the messaging platform and other protocols, such as Remote Method Invocation (RMI), IIOP and .NET remoting.	NA	Yes	[redacted]
41	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution will have the capability to work with security policy manager for Web services that allows for centrally defined security policies that govern Web services operations (such as access policy, logging policy, and load balancing).	NA	Yes	[redacted]
42	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have the capability to integrate with Master Data Management (MDM) technology for Enterprise Master Client Index (EMCI) implemented as part of the "State Hub" in a centralized or registry style implementation.	NA	Yes	[redacted]
43	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall be responsive and will automatically be sized for an optimum view to the display dimensions of PC, Tablet or Mobile phone.	NA	Yes	[redacted]

44	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution components will be committed to an advanced approach to interoperability using web services and Service Oriented Architecture (SOA) aligned with DHS Enterprise Architecture Standards and industry standards and vision for interoperability.	NA	Yes	[redacted]
45	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution must be architected to support replication of the virtual machines to a secondary site.	NA	Yes	[redacted]
46	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution must be designed so all releases can be performed between 7pm and 6am except critical releases	NA	Yes	[redacted]
47	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution shall leverage virtualization to expedite disaster recovery. Virtualization enables system owners to quickly reconfigure system platforms without having to acquire additional hardware.	NA	Yes	[redacted]
48	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution will provide the ability to perform archival/incremental backups and the ability to perform open/closed database backups.	NA	Yes	[redacted]
49	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution will provide at least one (1) production and one (1) non-production environment. Highly available solutions that mitigate single points of failure are recommended and encouraged.	NA	Yes	[redacted]

50	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall allow for different roles for Users including Operators, Administrators, Managers etc.	NA	Yes	[redacted]
51	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall, at a minimum, provide a mechanism to comply with security requirements and safeguard requirements of the following Federal agencies / entities: a. Health & Human Services (HHS) Centers for Medicare & Medicaid Services (CMS) b. Guidance from CMS including MITA Framework 3.0 and Harmonized Security and Privacy Framework c. Administration for Children & Families (ACF) d. Dept. of Agriculture Food and Nutrition Services e. NIST 800-53 r5 Moderate,	NA	Yes	[redacted]
52	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall adhere to the accessibility standard as outlined in the web guidelines and based on the W3C level 2 accessibility guidelines: (http://www.w3.org/TR/WCAG10/full-checklist.html)	NA	Yes	[redacted]
53	General System Behavior	Regulatory & Usability	Any technology vendor, application or solution shall adhere to the AR State accessibility standards and comply with the provisions of Arkansas Code Annotated § 25-26-201 et seq., as amended by Act 308 of 2013.	NA	Yes	[redacted]

54	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution comply with the DHS branding standards as defined by DHS.	NA	Yes	[redacted]
55	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall adhere to the principle of “Fail Safe” to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks	NA	Yes	[redacted]
56	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information	NA	Yes	[redacted]
57	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall follow the DHS Enterprise Architecture Standards regarding identity, authorization and access management. The current standards state that applications/solutions will integrate with Microsoft's Active Directory for internal/DHS users and will integrate with the IBM Cloud Identity platform for external users. Modern authentication protocols such as SAML or OIDC should be used and multi-factor authentication will be employed whenever deemed	NA	Yes	[redacted]

58	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall support protection of confidentiality of all Protected Health Information (PHI) and Personally Identifiable Information (PII) delivered over the Internet or other known open networks via supported encryption technologies needed to meet CMS and NIST requirements for encryption of PHI and PII data. Examples include: Advanced Encryption Standard (AES) and an open protocol such as Transport Layer Security (TLS), Secure Sockets Layer (SSL), Internet Protocol Security	NA	Yes	[redacted]
59	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall, when storing PHI/PII, support the use of encryption technologies needed to meet CMS and NIST requirements for the encryption of PHI/PII data at rest.	NA	Yes	[redacted]
60	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution, prior to accessing any PHI, display a State-approved configurable warning or login banner (e.g. "The System should only be accessed by authorized users"). In the event that a application or solution does not support pre-login capabilities, the application or solution will display the banner immediately following authorization.	NA	Yes	[redacted]

61	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall not transmit or store any Personal Health Information (PHI) or Personally Identifiable Information (PII) using publically available storage over the Internet or any wireless communication device, unless: 1) the PHI or PII is "de-identified" in accordance with 45 C.F.R § 164.514(b) (2); or 2) encrypted in accordance with applicable law, including the American Recovery and Reinvestment Act of 2009 and as required by policies, procedures and standards established by DHS	NA	Yes	[redacted]
62	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution will include the same security provisions for the development, System test, Acceptance test and training environment as those used in the production environment except those provisions implemented specifically to protect confidential information (e.g. PHI, PII).	NA	Yes	[redacted]
63	general System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall be able to associate permissions with a user using one or more of the following access controls: a. Role-Based Access Controls (RBAC; users are grouped by role and access rights assigned to these groups) b. Context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation-location, emergency-mode, etc.)	NA	Yes	[redacted]

64	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution will comply with accessibility requirements described in 45 CFR 85 and with State of Arkansas accessibility requirements	NA	Yes	[redacted]
65	General System Behavior	Solution Administration	Any technology vendor, application or solution will allow System administrators to create and manage user roles.	NA	Yes	[redacted]
66	General System Behavior	Solution Administration	Any technology vendor, application or solution communications will be protected by at least 256-bit encryption.	NA	Yes	[redacted]
67	General System Behavior	Solution Administration	Any technology vendor, application or solution will be supported by public key/private key encryption Secure Socket Layer (SSL) certificates.	NA	Yes	[redacted]
68	General System Behavior	Regulatory & Usability	Any application or solution will use colors to enhance user experience and System usability while complying with all disability requirements notated elsewhere in these requirements.	NA	Yes	[redacted]
69	General System Behavior	User Interrace	Any technology vendor, application or solution must perform address validation for demographic information (e.g., USPS, Smarty Streets, AR GIS, etc.). Suggest the validated new address and prompt user to select either user entered address or validated address and then save accordingly.	NA	Yes	[redacted]

70	General System Behavior	User Interface	Any technology vendor, application or solution must perform standard data validations such as character, numeric, date, currency , phone, SSN etc.	NA	Yes	[redacted]
71	General System Behavior	User Interlace	Any technology vendor, application or solution must have the ability to auto-save, prompt to save when leaving pages in all modules.	NA	Yes	[redacted]
72	General System Behavior	User Interlace	Any technology vendor, application or solution shall have the ability to create prompts for user actions. (e.g., incomplete data entry of required fields, deletion of data, system log-off warnings).	NA	Yes	[redacted]
73	General System Behavior	User Interlace	Any technology vendor, application or solution shall have the capability to send notifications. Examples include sending emails, text messages (SMS), etc.	NA	Yes	[redacted]
74	General System Behavior	Web based UI	Any technology vendor, application or solution providing data over a web browser interface (http, ftp, etc.) will include the capability to encrypt the data communicated over the network via SSL (e.g.. HTML over HTTPS).	NA	Yes	[redacted]

75	General System Behavior	Web based UI	The system will support and maintain compatibility with the current to (N-2) version of the DHS Support Operating Systems. The supported Operating Systems are Microsoft Windows, MAC OS, Apple IOS and Google Android.	NA	Yes	[redacted]
76	General System Behavior	Web based UI	The system will support and maintain compatibility with the current to (N-2) version of the DHS approved Browsers. The supported Browsers are Chrome, Edge, and Safari. This is to ensure that vendors test and certify their software/application for current to (N-2) versions of these Browsers.	NA	Yes	[redacted]
77	Technology Platform Requirements	Data Integ,Quality, ETL	Any technology vendor, application or solution Extract Transform and Load (ETL) components will provide process flow and user interface capabilities to enable business users to perform data-quality-related tasks and fulfill stewardship functions, including: a. Packaged processes, including steps used to perform common quality tasks (providing values for incomplete data, resolving conflicts of duplicate records, specifying custom rules for merging records, profiling, auditing, for example) b. User interface in which	NA	Yes	[redacted]

Requirement Number	Category	Comment for consideration
1	Application/Solution Hosting	DHS is interested in seeing the following hosting options for any new procurements: 1) On-Premise 2) Private Cloud 3) Hybrid Cloud 4) Public Cloud 5) SaaS, PaaS or other emerging options
2	Application/Solution Hosting	When proposing cloud, private cloud, or hybrid cloud solutions, respondents should make sure to clearly identify provisions, terms, conditions and details around the following areas: 1) Cost 2) Performance 3) Data Management 4) Governance 5) Service Levels 6) Location of Data 7) Vendor obligations in the event of a data breach 8) Provisions for data export and exit strategy 9) Provisions for data destruction by vendor after contract termination 10) Data Security 11) Regulatory compliance 12) Change processes and procedures 13) Information access costs/requirements (i.e. FOIA request, etc.)
	Data	DHS would prefer for all data to be encrypted using the latest/supported technology protocols whether at rest/stored, in flight/transit, or communicated and/or accessed in any way.

Attachment I
REVISED Client History Form
Arkansas Health Insurance Premium Payment
RFP # 710-24-0002

Attachment I

Arkansas Health Insurance Premium Payment (ARHIPP) Client History Form

Instructions: This form is intended to help the State gain a more complete understanding of each Respondent's Medicaid Program experience. This form **must** be completed completely and accurately.

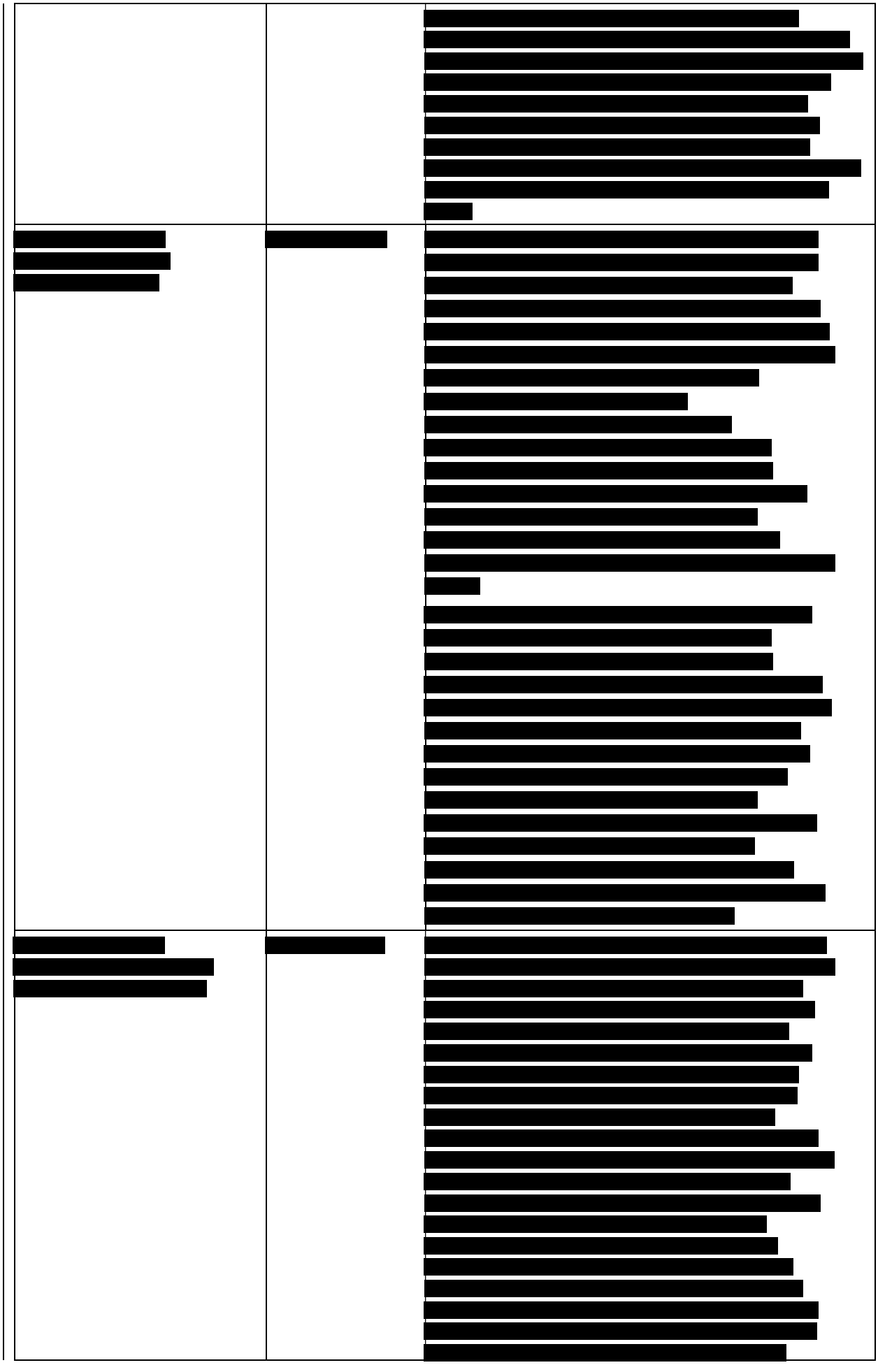
The State reserves the right to verify the accuracy of these answers by contacting any of the listed clients, and all applicable clients **must** be listed. Omission of a client will constitute a failure to complete this form.

For purposes of this form, the "client" is not an individual but the entity which held the contract. By way of explanation, in the Contract resulting from this RFP, Arkansas DHS will be the client. For each listed client, Respondents may (but are not required) provide the contact information for a person at the client entity who is knowledgeable of the named project. If the State contacts clients listed on this form, the State reserves the right to contact the listed individual or another person at the listed client.

The boxes below each prompt will expand if necessary. The form **must** be signed (please see the final page) by the same signatory who signed the Proposal Signature Page.

1. Please list at least three (3) clients (federal, district, state, county, American territory, tribe, or Canadian province) for whom you (the prime contractor only) **served as the prime contractor** on similar insurance contracts for other state Medicaid programs for at least five (5) years . For each client, please specify the organization/agency/division, not just the state or political subdivision. Please briefly describe the scope of the contract. If there are no contracts which meet this definition, please state "none."

Client Name (Organization /Agency/Division)	Years (201x)	Scope Description
[redacted]	[redacted]	[redacted]



[redacted]

2. Please list at least three (3) clients (federal, district, state, county, American territory, tribe, or Canadian province) where a **proposed subcontractor served as the prime contractor** on similar insurance contracts for other state Medicaid programs for at least five (5) years. For each client, please specify the organization/agency/division, not just the state or political subdivision. Please briefly describe the scope of the contract. If there are no contracts which meet this definition, please state "none."

No subcontractor proposed.

Authorized Signature: [redacted]

Printed/Typed Name:

INFORMATION FOR EVALUATION

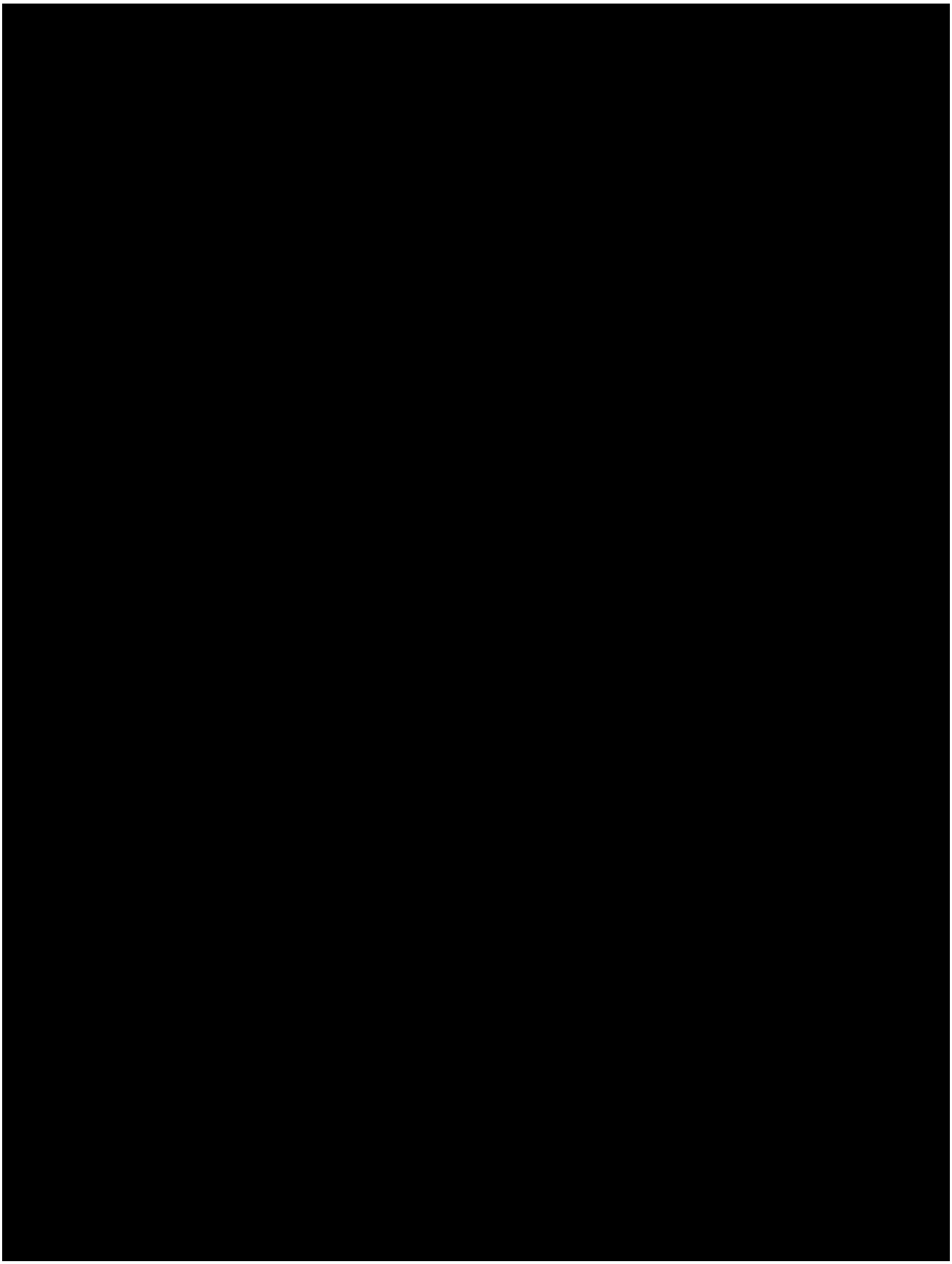
- *Provide a response to each item/question in this section. Prospective Contractor may expand the space under each item/question to provide a complete response.*
- ***Do not** include additional information if not pertinent to the itemized request.*

E.1 General Requirements

ITEM/QUESTION

A. Describe your process for determining eligibility for the ARHIPP program.

[redacted]



[redacted]

[redacted]

[redacted]

ITEM/QUESTION

B. Describe your policies and plans for ensuring your company does not practice discriminatory selection among eligible Beneficiaries, including not excluding, seeking to exclude, or otherwise discriminating against any group or class of individuals.

[redacted]

[redacted]

ITEM/QUESTION

C. Describe your process for verifying the ARHIPP applicant's insurance policy information.

[redacted]

[redacted]

ITEM/QUESTION

D. Describe your process for re-determining ARHIPP eligibility for all active cases prior to the end of the employer's open enrollment periods.

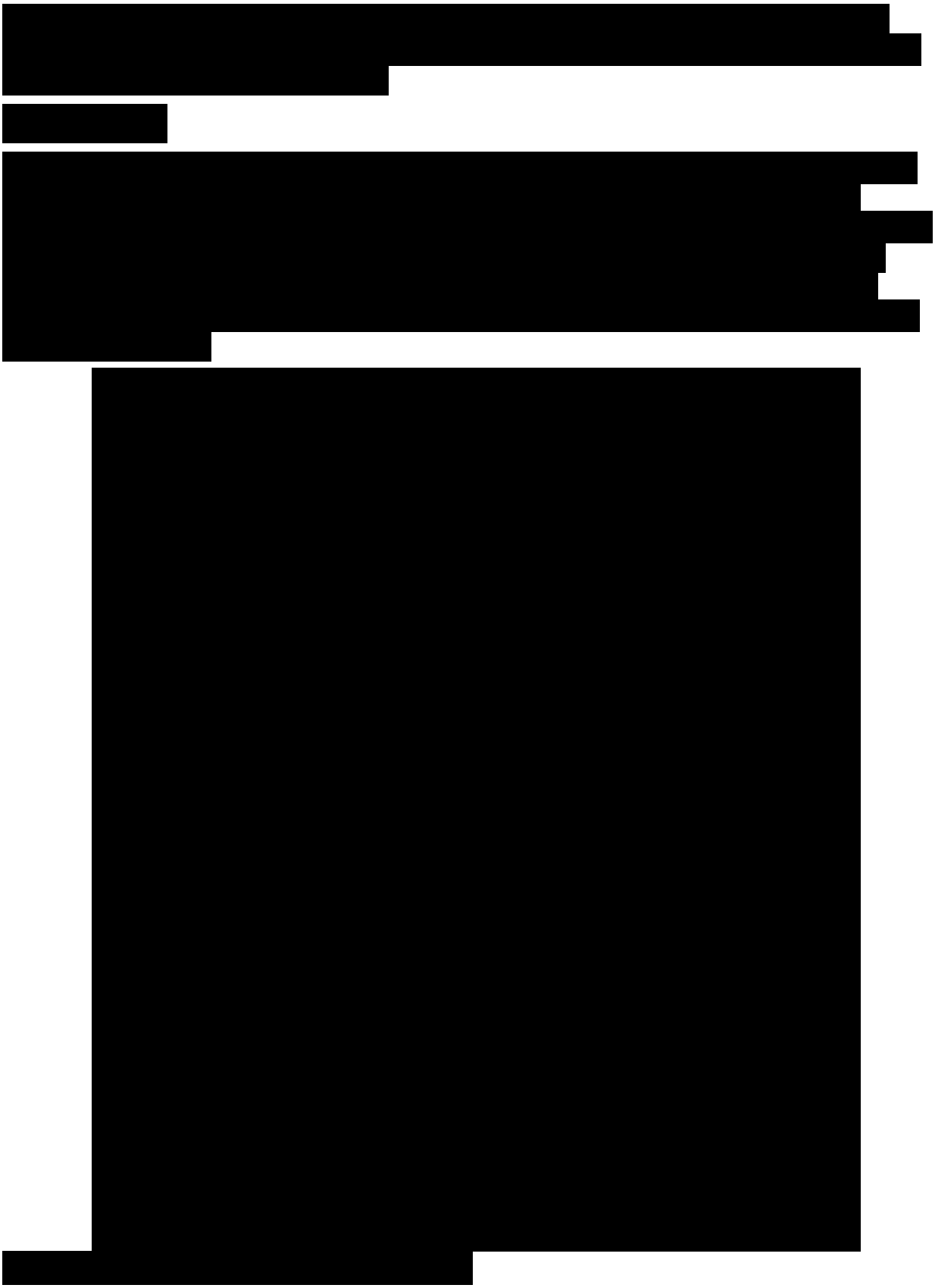
[redacted]

[redacted]

ITEM/QUESTION

E. Describe your process for using the eligibility data contained in the TPL file to update existing ARHIPP cases and establishing new cases.

[redacted]



[redacted]

[redacted]

ITEM/QUESTION

F. Describe your plan for monitoring the timeliness of the notice delivery process.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

ITEM/QUESTION

G. Describe your plan for checking the third party liability status before payments are made.

[redacted]

[redacted]

ITEM/QUESTION

H. The State is interested in automating as many processes as possible. Describe your plan for automating as many of the processes and to the greatest degree possible outlined in Section 2.4.A of the RFP.

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

ITEM/QUESTION

I. The State is also interested in mitigating increasing administrative costs year over year. Describe your plan to increase efficiency and minimize increasing costs.

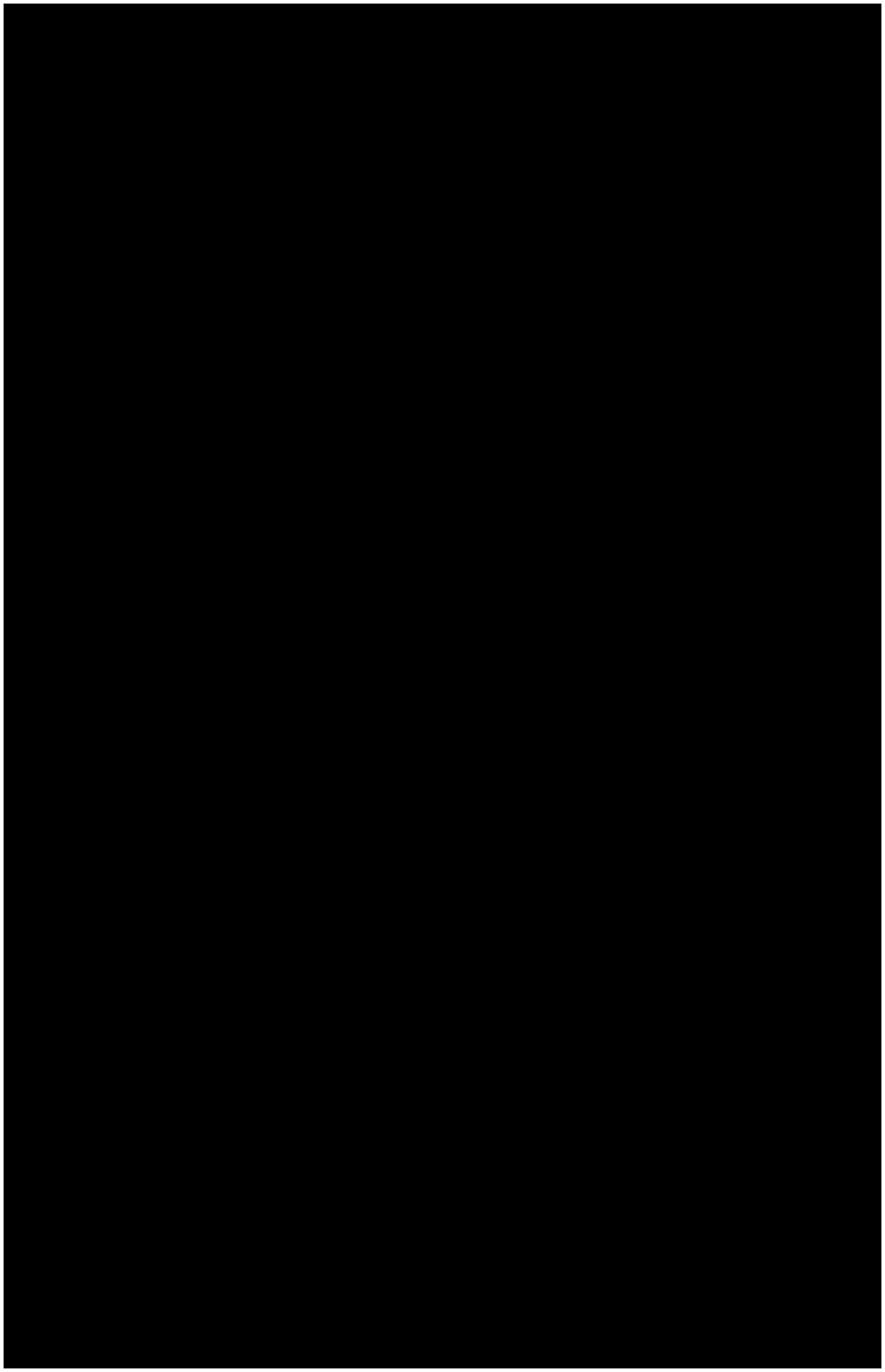
[redacted]

[redacted]

ITEM/QUESTION

J. Describe your methodology for determining beneficiaries' cost-effectiveness for the ARHIPP program in accordance with the Promulgated rules of the AR Health Insurance Premium Policy.

[redacted]



E.2 CALL CENTER REQUIREMENTS

ITEM/QUESTION

A. Describe your plan for installing, operating, monitoring, and supporting an Automated Distribution Call (ADC) system and performing the general Call Center requirements listed in the RFP.

[redacted]

[redacted]

ITEM/QUESTION

B. Describe your plan for operating a HIPAA-compliant, toll-free Call Center per the requirements of the RFP, and whether you intend to operate the Call Center for Beneficiaries and Providers separately or combined.

[redacted]

[redacted]

ITEM/QUESTION

C. Describe your process for handling calls received outside of normal business hours.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

ITEM/QUESTION

E. Describe your technological capability for auditing and monitoring calls and your process for implementing and utilizing an electronic system to document calls and use the data for reference, tracking, and analysis.

[redacted]

ITEM/QUESTION

F. Describe your electronic system for documenting calls.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

ITEM/QUESTION

G. Provide your Call Center Disaster Recovery Plan

- **Does the plan Include annual testing**
- **Does the plan indicate sharing results with DHS**
- **Does the plan indicate how any deficiencies will be listed and how corrective actions will be remediated**

[redacted]

[redacted]

[redacted]

[redacted]

ITEM/QUESTION

[redacted]

[redacted]

ITEM/QUESTION

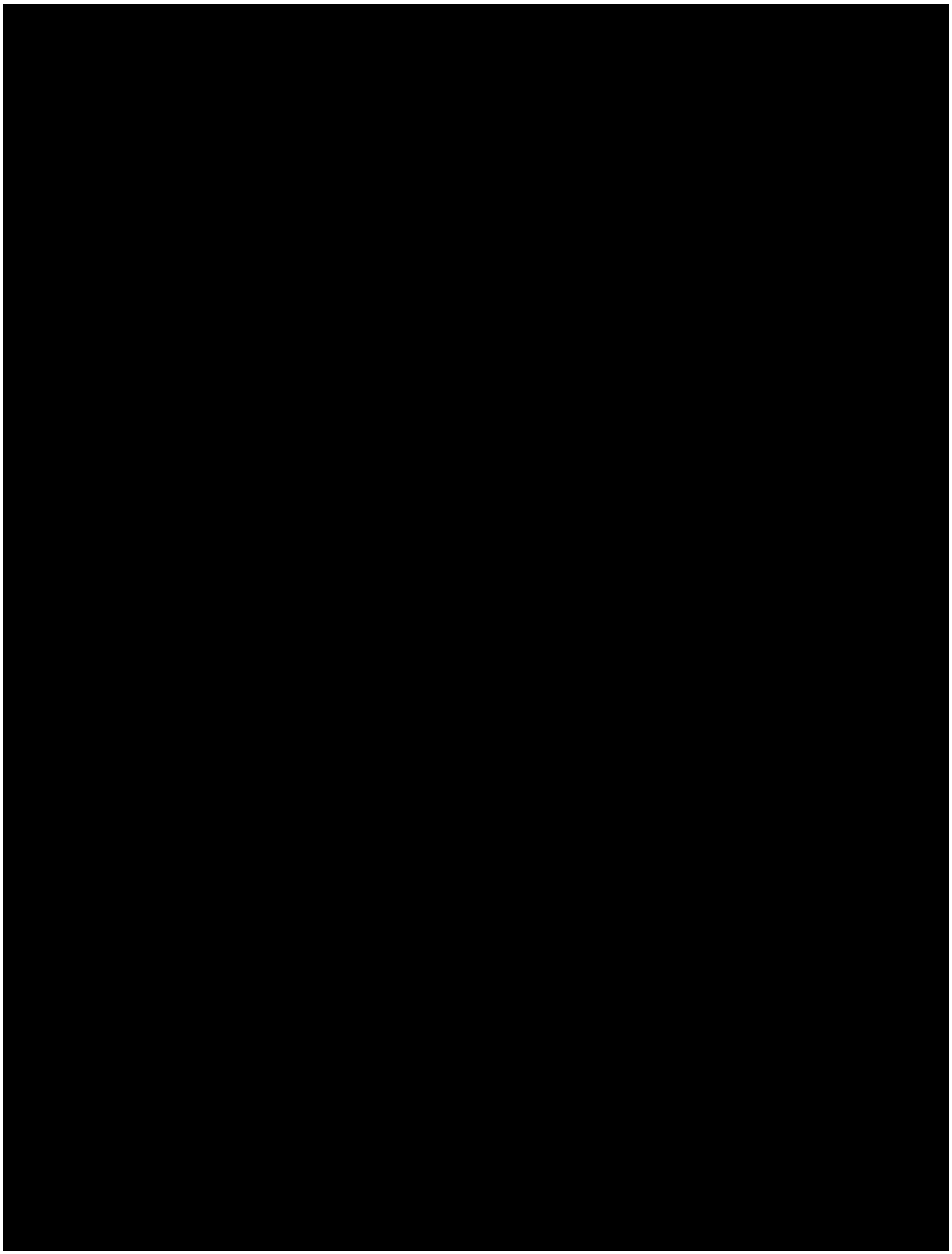
I. Describe your process for keeping an electronic record of all Grievances received by the Call Center.

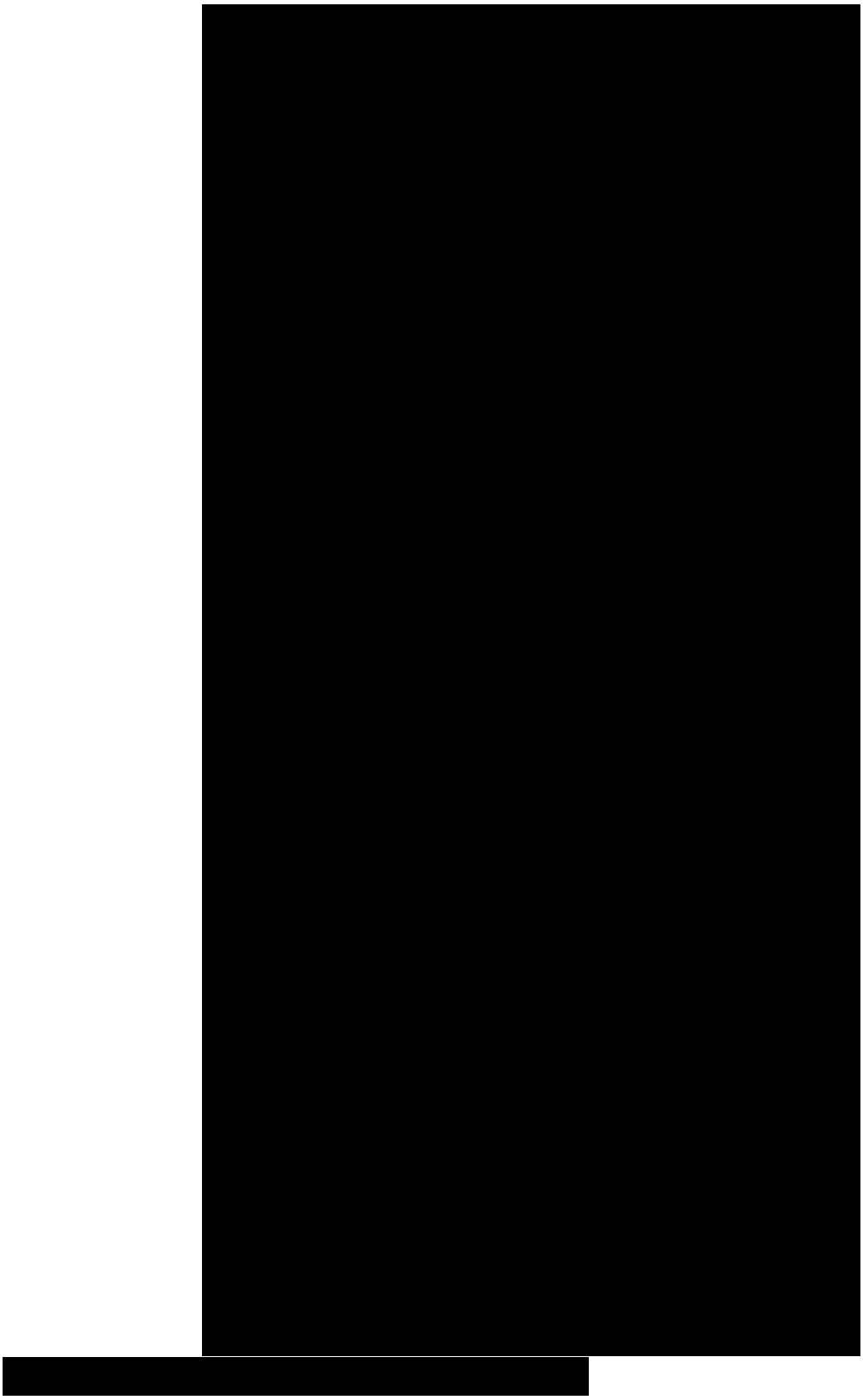
[redacted]

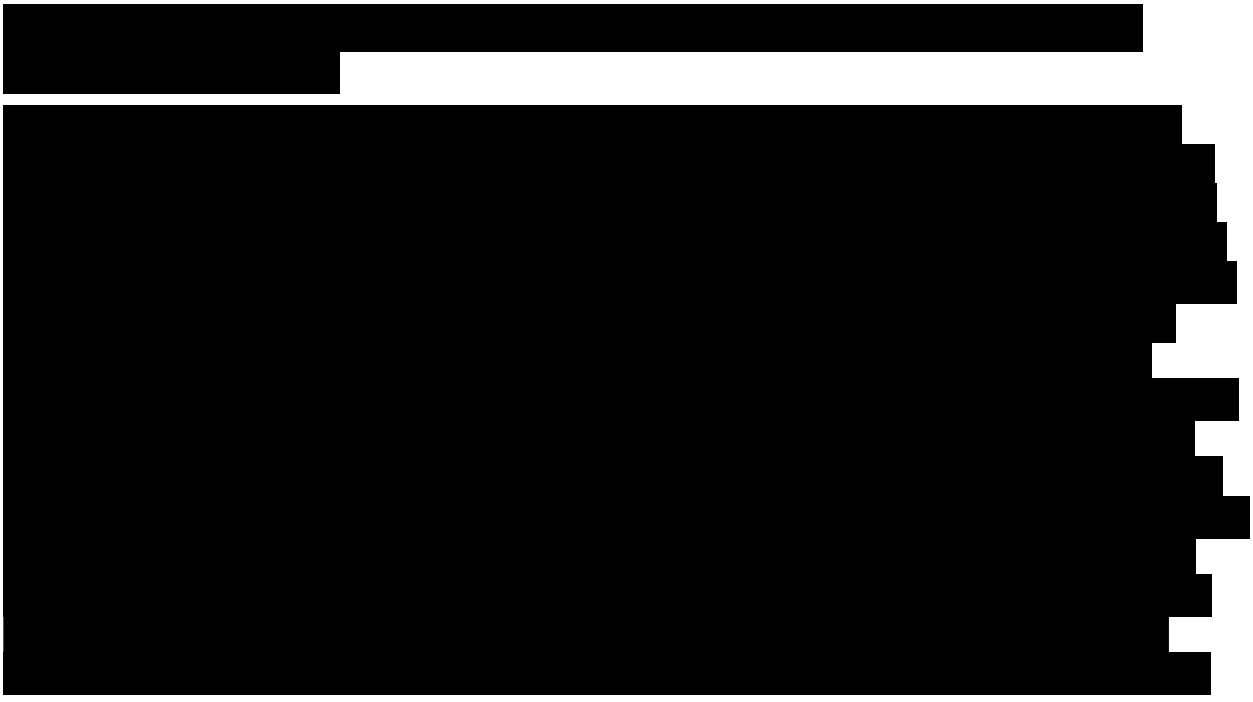
ITEM/QUESTION

J. Describe your plan for developing and maintaining a website with separate pages for Beneficiaries that is easy to access, user-friendly, and compliant with the required items in the RFP.

[redacted]







ITEM/QUESTION

K. Describe your plan for implementing and maintaining secure electronic portals for Beneficiaries on the website.

[redacted]

[redacted]

[redacted]

ITEM/QUESTION

L. Describe your plan for ensuring information on the website is accurate and for ensuring the information is updated in a timely manner, defined as at least monthly in the RFP and more frequently if needed.

[redacted]

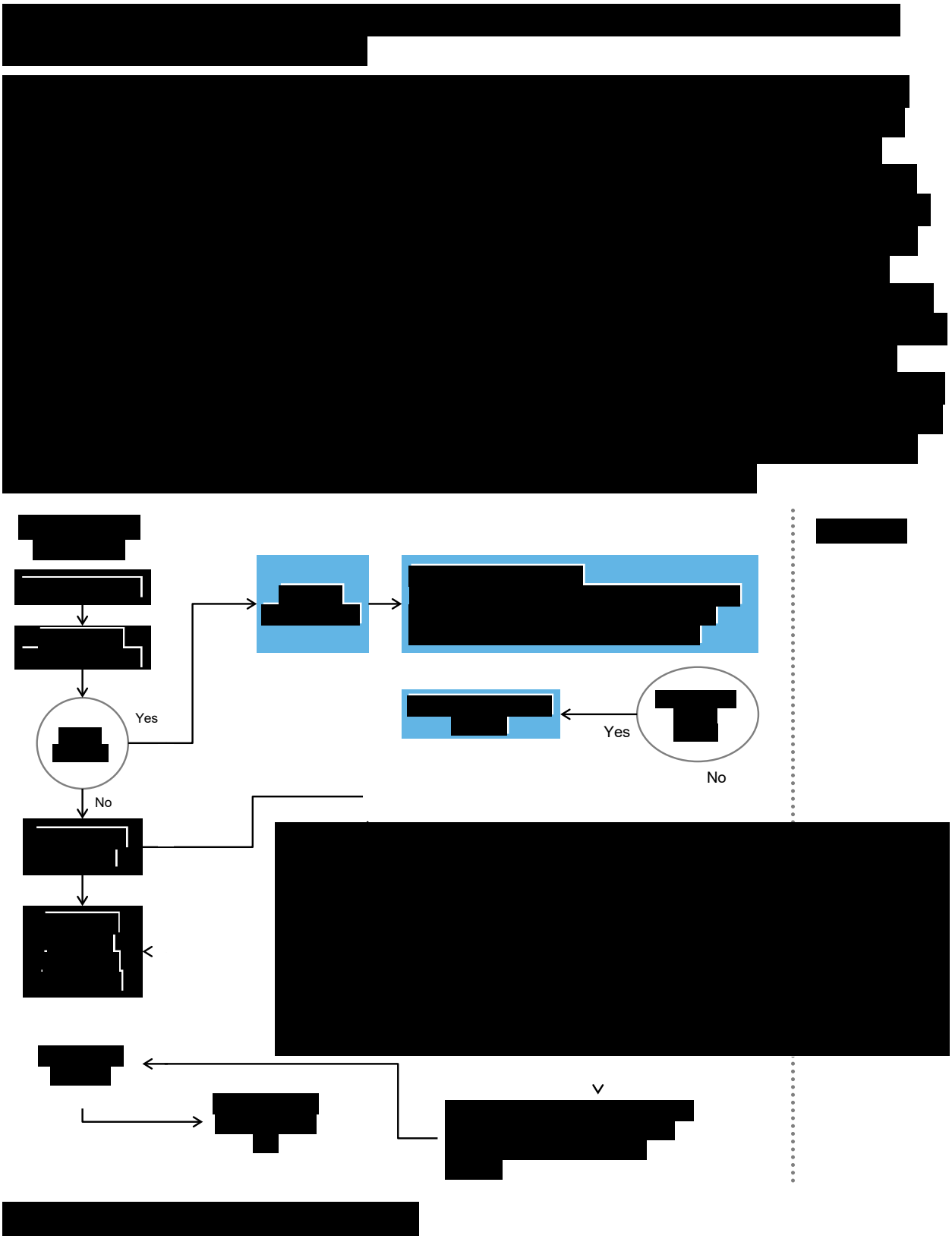
E.3 Administration

ITEM/QUESTION

A. Describe your plan for development, maintenance, operations, and administration of the ARHIPP Program.

[redacted]

[redacted]


Yes
No
Yes
No

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

ITEM/QUESTION

B. Describe your plan for maintaining an organizational structure and staffing levels to administer the ARHIPP Program.

[redacted]

[redacted]

ITEM/QUESTION

C. Describe in detail how the proposed Key Personnel's experience and qualifications relate to services outlined in this RFP.

[redacted]

[redacted]

ITEM/QUESTION

D. Describe your plan for substitution or replacement of Key Personnel.

[redacted]

[redacted]

ITEM/QUESTION

E. Describe your plan for developing and implementing training and materials for all staff, including subcontractors.

[redacted]

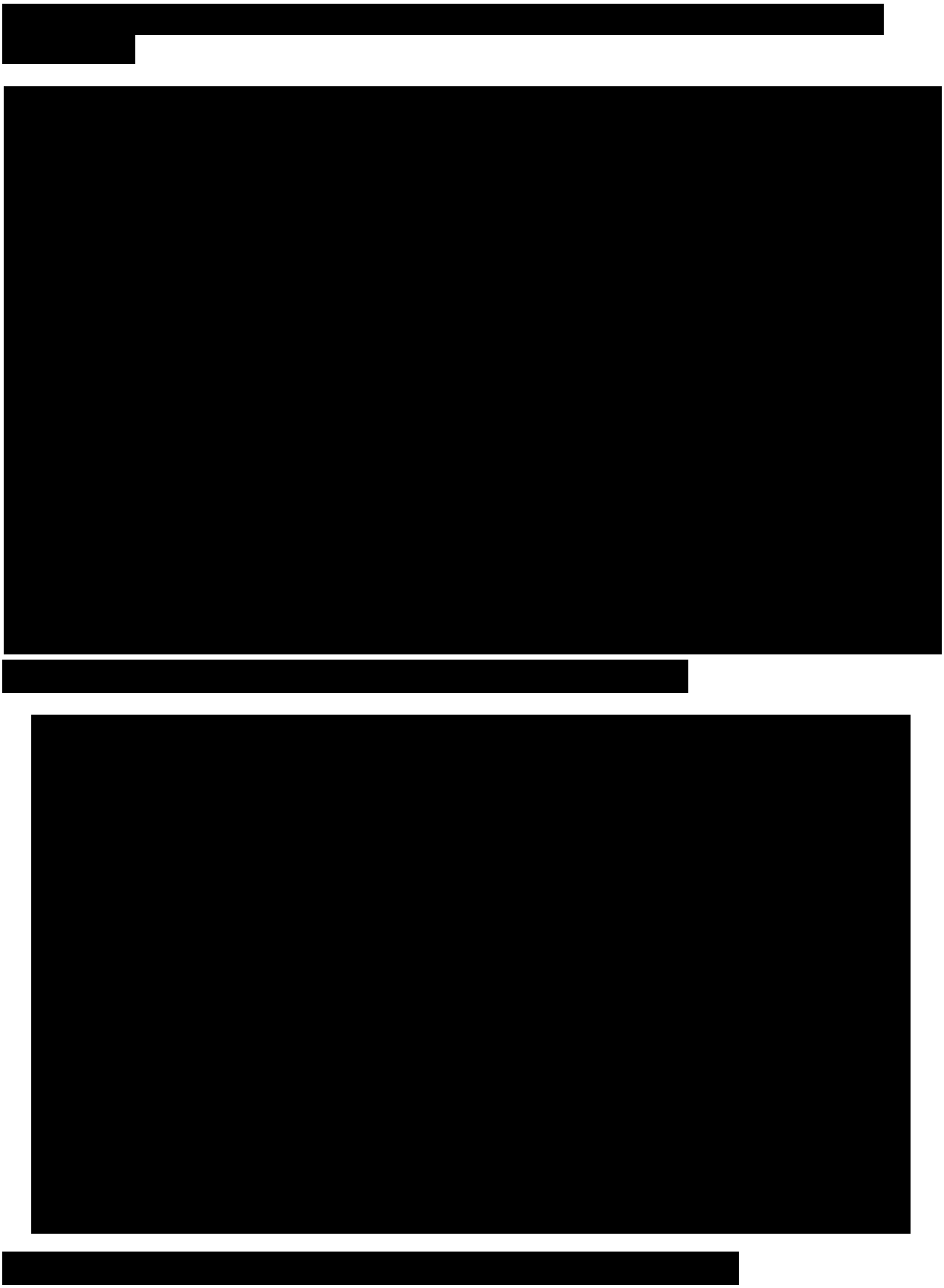
[redacted]

E.4 Reporting

ITEM/QUESTION

A. Describe your plan for generating reports and capturing all information outlined in the RFP.

[redacted]

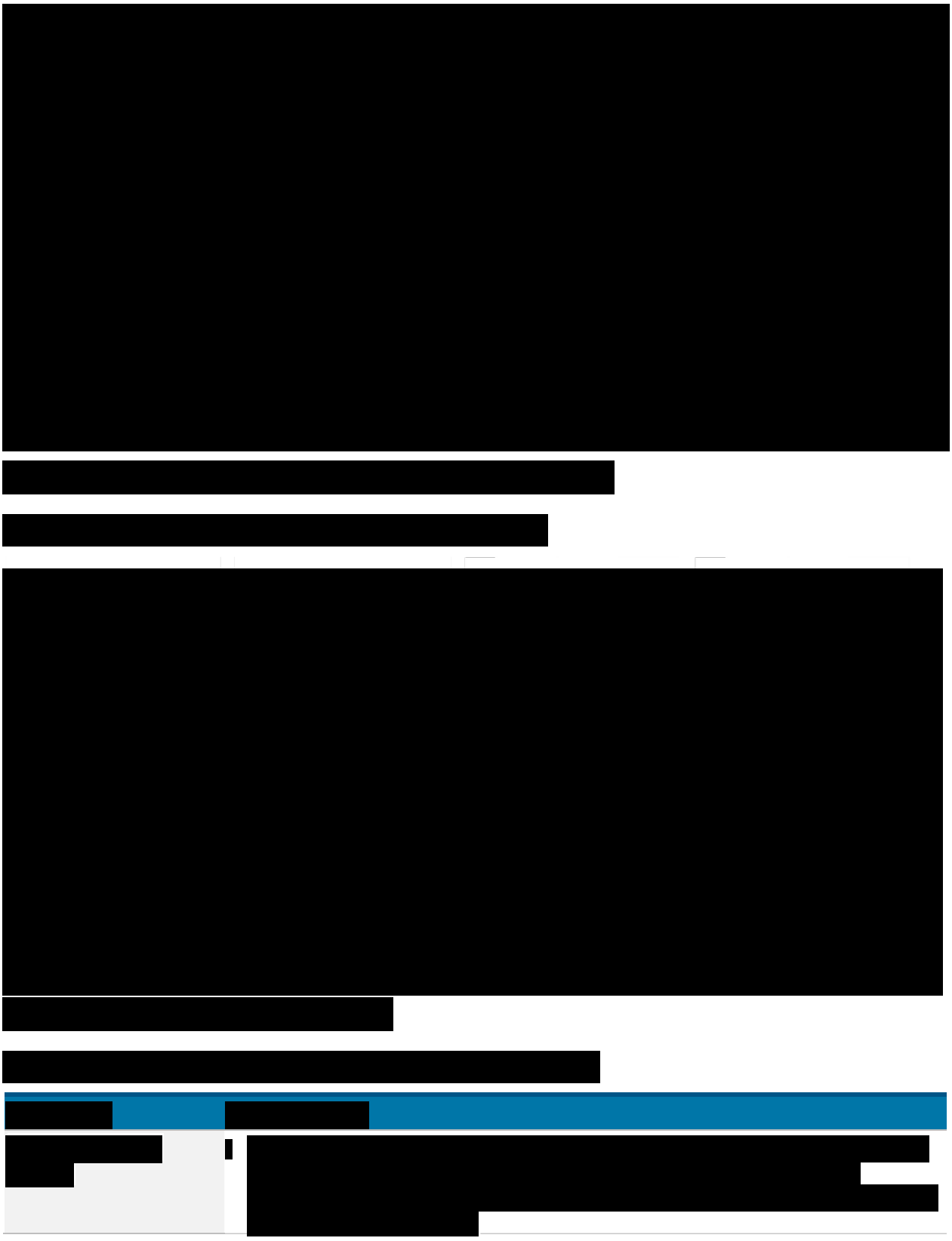


[redacted]

ITEM/QUESTION

B. Describe your ability to generate and provide ad hoc reports within the timeframe specified by DHS.

[redacted]



[redacted]

ITEM/QUESTION

C. Describe your plan for optimizing reporting capabilities to allow the State to generate various timely reports as needed.

[redacted]

E.5 System Security & Privacy

ITEM/QUESTION

A. Please state your understanding of the latest versions of 45 CFR 164.522(b), NIST SP 800-53 Rev. 5 , MARS-E 2.2, and explain how your Solution will ensure that these requirements are met. In your answer, please describe how your Solution can manage confidential data.

[redacted]

[redacted]

ITEM/QUESTION

B. Describe all privacy and security incidents (i.e., a breach, improper disclosure) affecting the information of individuals that have occurred in systems implemented or maintained by the Respondent (its subsidiaries and affiliates) or any subcontractor within the past five years. Describe how you handled the incident(s).

[redacted]

ITEM/QUESTION

C. Provide a proposed System Security Plan in accordance with the details outlined in RFP Section 2.5.

[redacted]

ITEM/QUESTION

D. Describe how your proposed Solution will protect sensitive information, including but not limited to Client information and Provider information.

[redacted]

[redacted]

ITEM/QUESTION

E. How will you ensure security and confidentiality of information, while allowing for a free flow of information accessible through various means?

[redacted]

ITEM/QUESTION

F. Does the contractor perform an annual Penetration Test and provide DHS with the RAW results

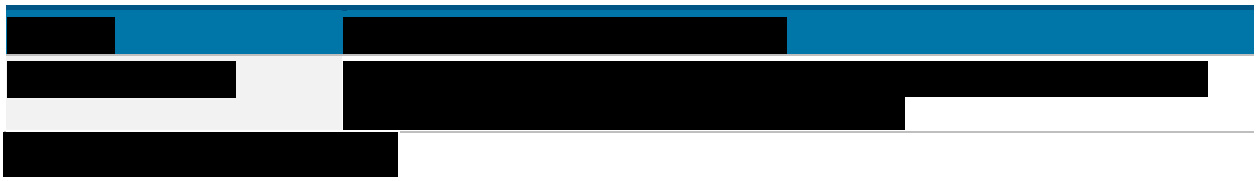
[redacted]

E.6 Information Management and Systems

ITEM/QUESTION

A. Describe your Information Technology platform and plan for the management and administration of ARHIPP and its ability to interact and exchange data electronically including MMIS.

[redacted]



[redacted]

[redacted]

ITEM/QUESTION

B. Describe your plans for developing and maintaining your management information system.

[redacted]

[redacted]

[redacted]

ITEM/QUESTION

C. Describe your plan for providing for varying levels of access based on role for Contractor and State staff.

[redacted]

ITEM/QUESTION

D. Describe your IT Platform's ability to customize reporting.

[redacted]

[redacted]

ITEM/QUESTION

E. Describe your IT Platform's capability to directly interface with the MMIS and support direct electronic interaction with DHS's system.

[redacted]

ITEM/QUESTION

F. Describe your plan for providing varying levels of access based on roles.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

ITEM/QUESTION

G. Describe the process for completing address validation prior to communicating with beneficiaries.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

ITEM/QUESTION

H. Describe your process for identifying deficiencies requiring system updates or changes.

[redacted]

ITEM/QUESTION

I. Describe your approach and methodology for compliance with ADA 508 – Web Content Accessibility Guidelines (WCAG).

E.7 Disaster Recovery and Business Continuity

ITEM/QUESTION

A. Describe your Disaster Recovery Plan for the claims processing system

- **Does the plan Include annual testing**
- **Does the plan indicate sharing results with DHS**
- **Does the plan indicate how any deficiencies will be listed and how corrective actions will be remediated**

[redacted]

ITEM/QUESTION

B. Describe your system's protection against hardware and software failures, human error, natural disasters, and other emergencies that could interrupt services.

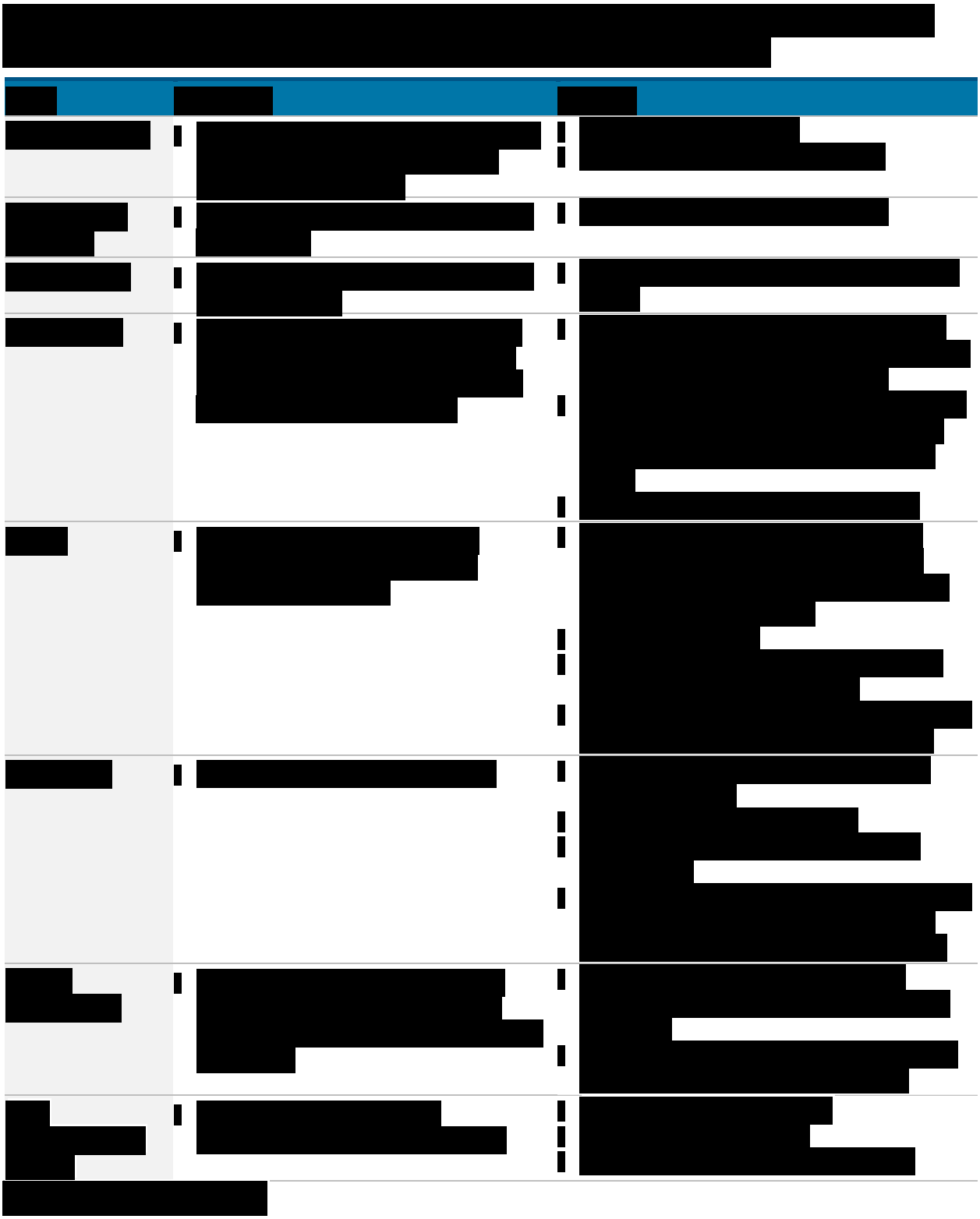
[redacted]

E.8 Transition and Implementation

ITEM/QUESTION

A. Provide and describe key milestones for IT development and implementation.

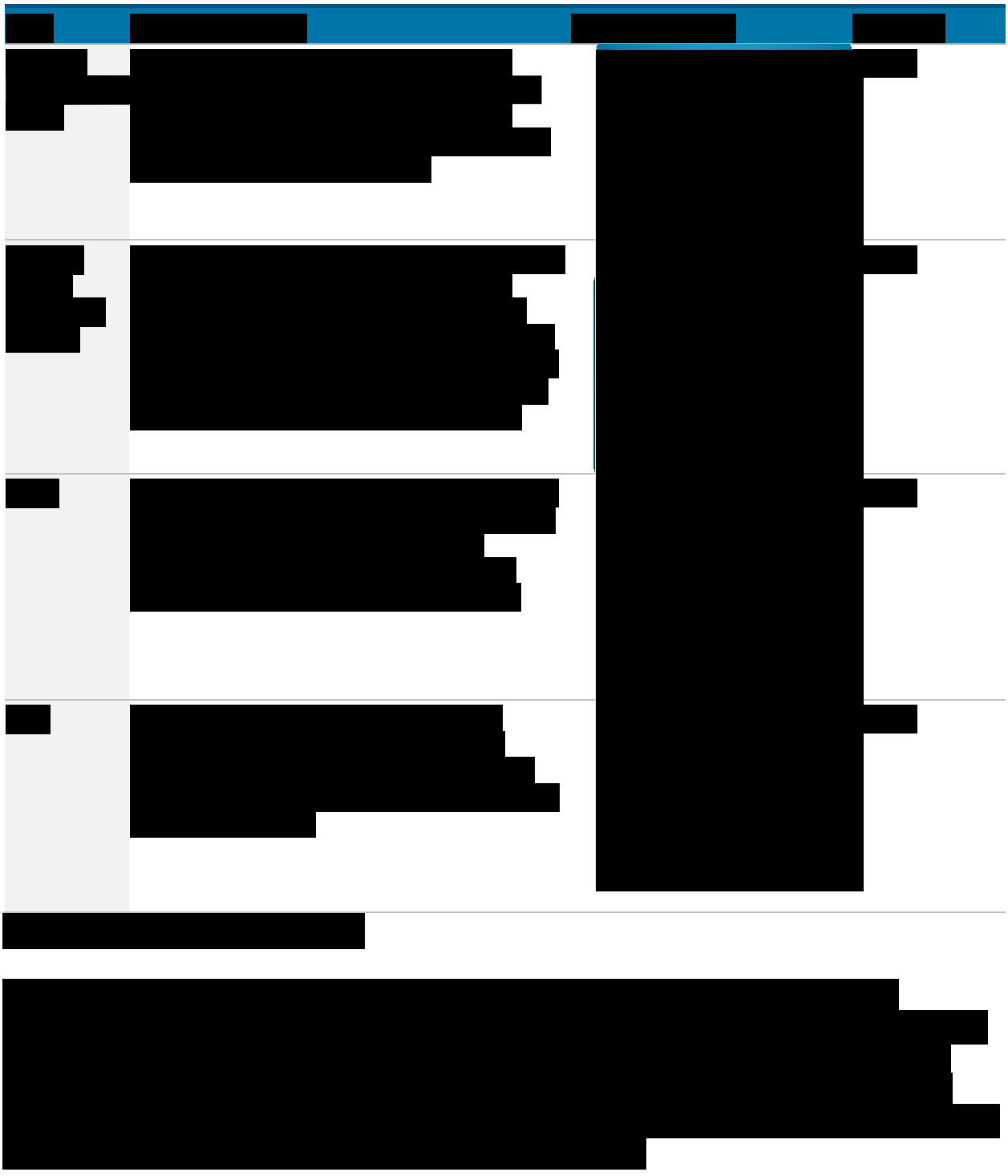
[redacted]



ITEM/QUESTION

B. Describe your implementation report structure to keep the State apprised of implementation efforts and the content and frequency of all required reports.

[redacted]



ITEM/QUESTION

C. Describe your policies and plans for ensuring your company does not practice discriminatory selection among eligible Beneficiaries, including not excluding, seeking to exclude, or otherwise discriminating against any group or class of individuals.

[redacted]